Council of the European Union
General Secretariat

Interinstitutional files:
2018/0331(COD)

Brussels, 23 November 2018

WK 14512/2018 INIT

LIMITE

ENFOPOL
COTER
JAI
CYBER
TELECOM
FREMP
AUDIO
DROIPEN
CODEC
CT

WORKING PAPER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From: To:	General Secretariat of the Council Working Party on Terrorism
N° prev. doc.:	WK 12386/18; WK 12931/18; WK 13690/18; WK 14189/18; WK 14291/18
Subject:	Compilation of additional comments submitted by delegations on the Proposal for a Regulation on preventing the dissemination of terrorist content online

Delegations will find in Annex a compilation of additional comments on the Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online.

Contents

Germany

1. Journalistic/editorial content

We thank the Presidency for amendments in the recitals regarding freedom of the press and pluralism of the media. But we are not sure if this enough to ensure that journalistic/editorial content hosted on third-party platforms may not be subject to removal orders. We therefore propose adding an explicit exception for content that is attributable or disseminated under the editorial responsibility of a provider governed by standards in line with Union Law to the definition.

Text proposal:

Article 2 paragraph 5:

"In terms of this regulation 'terrorist content' shall not mean content published under the editorial responsibility of a content provider based on journalistic standards established by press or media regulation consistent with the law of the Union."

2. Relation Article 4 and Article 5

We believe the relation between articles 4 and 5 requires further clarification (at least in the recitals): According to the principle of proportionality, pursuant to Article 4 the competent authority may, as a rule, issue a removal order only after it has sent a referral to the hosting service provider informing it of the terrorist content pursuant to Article 5 or in cases of immediate threat to life or to national security.

Proposal

Recital 15:

The referral mechanism of alerting hosting service providers to information that may be considered terrorist content, for the provider's voluntary consideration of the compatibility with its own terms and conditions, constitutes an particularly effective, swift **and proportionate** means of making hosting service providers aware of specific content on their services **especially in cases where the hosting service provider has not been misused before or when it has taken sufficient action on referrals except in cases of immediate threat to life or in cases of a threat to national security**.

Or Article 4 new paragraph 1a:

"If the hosting service provider has not been misused for disseminating terrorist content before or takes sufficient action on referrals under Article 5, a removal order may be appropriate in cases of immediate threat to life or in cases of threat to national security."

3. Relation between the proposed regulation and the e-evidence package / EPOC Regulation:

Regarding the relation between criminal investigations and removing content, the key question is what should be done when EPOC or prior criminal investigations in one EU member state collide with removal orders of another EU member state. When online content is taken down following a removal order, this may alert the content provider and could interfere with possible undercover investigations. For such cases, a participation mechanism of the member states affected by a removal order seems necessary so that they could intervene in the process if necessary. We are strongly supportive of the role of Europol for coordination and de-confliction regarding removal orders and referrals. But we think there should also be a provision in the text addressing the conflict.

Text proposal:

Article 4 new paragraph 9:

"If the removal order concerns content data and this data have already been requested via an European Production or Preservation Order for electronic evidence in criminal matters, the addressed hosting service provider shall inform the competent authority without undue delay about the competing orders. The competent authority shall thereupon, as soon as possible, liaise with the authority having issued the European Production or the European Preservation Order in order to clarify which Order should be given priority by the hosting service provider. The deadline set out in paragraph (2) shall apply as soon as the competent authority issuing the removal order confirms the priority of the removal order."

Article 5 new paragraph 8:

"If the referral concerns content data and this data have already been requested via an European Production or Preservation Order for electronic evidence in criminal matters, the proceeding pursuant to Article 4 (9) shall apply."

4. Legal remedy for content providers to contest a removal order

We believe that legal remedy in case of removal orders must be explicitly governed in the main text of the regulation, as in Article 10 for referrals and proactive measures, and not only in a recital (Recital 8).

Text proposal

Article 10 new paragraph 3:

"Hosting service providers and content providers whose content has been removed following a removal order pursuant to Article 4 have a right to effectively contest the removal order before the court of the Member State whose authorities issued the removal order. Due information on the relevant legal remedies shall be provided by that Member State upon request of the hosting service provider or content provider."

5. Jurisdiction and Enforcement (Article 15)

To avoid any misunderstanding about jurisdiction for enforcement of removal order Germany would welcome a clarification in recital 38.

Proposal:

"The enforcement of a removal order is subject to the relevant provisions of a mutual legal assistance agreement and to the relevant national law of the Member State in which the main establishment of the hosting service provider is located."

Estonia

Article 18 and recital 38.

We are unsure of the addition of the sentence in recital 38 that goes with Article 18 regarding taking into consideration any coercive measures taken when imposing penaties for non-compliance of a removal order – has this option not been eliminated in Article 15?

Recital 34/Article 15

We appreciate the clarifications in paragraphs 1 and 2, which has made the question of jurisdiction much clearer.

We are also happy to see the removal of paragraph 3, as we did not understand how it would be possible to enforce the non-punitive coercive measure itself if the HSP is located in another MS and refuses also to comply with the non-punitive coercive measure.

So do we now understand correctly, that only the host MS would have jurisdiction under Article 18(1)(b) to impose a penalty on the HSP for failure to implement the removal order issued by the other MS?

We are unsure particularly because of the addition of the sentence in recital 38 that goes with Article 18 regarding taking into consideration any coercive measures taken when imposing penalties for non-compliance of a removal order – has the option of a coercive measure imposed by the MS that issued the removal order not been eliminated in Article 15?

This has only solved one problem. We still have the problem of how hosting service providers and content providers will be able to effectively protect their rights if they have to contest a removal order in another Member State.

Art 13 dealing with the cooperation (and recitals 27-31)

No comments

In addition art 18.

We share NL concerns about the system of cross-border removal orders and its implications for an effective legal remedy. However, NL proposal to allow all MS to issue removal orders but have any disputes be under the jurisdiction of the host Member State is also problematic. While it would be more beneficial for the hosting service provider and the content provider to be able to contest a removal order in the jurisdiction with which they are familiar, it is hard to imagine how the courts in for example Estonia would be able to resolve a dispute about an administrative decision taken in for example Portugal.

Greece

Dear colleagues,

following today's meeting and in view of the preparation of the revised document, please be informed that we would like to reiterate our proposal for recital 13a. Specifically, we would like to include national security to the sensitive information referred to in that Recital in order to clarify that sensitive information do not only include on-going investigation data. We propose the following amendment to recital 13a: [...]The reasons provided need not contain sensitive information which are related to its national security or could jeorpardise investigations. [...]

Finally, we would like to support the Presidency's amendment on Article 24 (12-month period for application) which takes into account the different level of preparedness in Member States, both on legislative and on operational terms.

France

The French authorities express their satisfaction with the text submitted by the Commission. This project meets their expectations regarding the core of the text; they are therefore prone to make a constructive contribution to the debates in order to facilitate their progress, with a view to adopting the text in the first quarter of 2019.

In this context, the French authorities wish to make the following observations which aim at further enriching this proposal:

Recitals 12 and 17

The French authorities would like to clarify recitals 12 and 17 in order to avoid suggesting that the text would legitimize the maintenance of illegal content for reasons other than terrorist.

Thus, they suggest that the third sentence of recital 12 and the second sentence of recital 17 be supplemented by the words *"in order to avoid unwanted and erroneous decisions leading to the deletion of content which is not terrorist in character* ***and which is not illicit****"*.

Article 15 and Recital 34: Jurisdiction

The French authorities wish to retain paragraph 3, which specifies that each Member State remains competent to take coercive measures to ensure the implementation of its removal orders.

Indeed, granting the Member States the power to require the removal of terrorist content online only makes sense if those same States can sanction the lack of knowledge of these orders. Failing this, the mechanism provided for in Article 4 would only be of use to Member States with the capacity to enforce their decisions, i.e. the Member State in which the hosting service provider have its principal establishment.

The reinstatement of paragraph 3 is therefore necessary to preserve the possibility for Member States to issue removal orders against hosting service providers not having their principal place of business in their territories. This possibility is one of the key points of the European Commission's proposal. It is the counterpart of the attribution of the general competence to regulate the action of the content providers, not for the Member States whose population is targeted by these operators, but for the Member State hosting their main establishments. The adoption of the regulation without Article 15, paragraph 3, would therefore greatly unbalance the proposed text.

In addition, such a regulation would represent a significant step back from the current legislation in those Member States which already have supervisory authorities, like France. The French supervisory authority would lose the power to enforce the removal orders it can issue against hosting service providers having their principal place of business in other Member States. For the record, non-compliance with these orders by a legal person is now sanctioned in French law by a fine of 375,000 euros.

In view of the discussion of Article 15 (3), the reinstatement of this paragraph as originally proposed by the European Commission appears to be the most balanced solution.

Moreover, the French authorities do not support the Dutch proposal set out in WK 14189/2018 INIT of 20 November adding a fourth paragraph to Article 15 conferring jurisdiction on the courts of the Member State which has jurisdiction to examine applications for damages about removal orders from other Member States. That would lead to the judgment of a decision taken by a public authority of a Member State pursuant to its prerogatives of public authority by the courts of another Member State. This provision would be contrary to public international law and the constitutional provisions of many Member States, including France.

Article 18 and Recital 38: Penalties

The French authorities welcome the reformulation of recital 38 which offers guarantees of proportionality.

Without making it a blocking element, they wish to rephrase their proposal to define a minimum threshold for the maximum penalty incurred.

In order to avoid a dumping effect between Member States, the French authorities propose to define a penalty in paragraph 4 as being able to reach 2 to 4% of the overall turnover for the previous financial year.

In addition, the French authorities recall their point of view on the concept of a harmonized sanctions mechanism in order to ensure the non-appearance of a phenomenon of dumping between Member States. The fact that the sanction is harmonized at Member State level is a counter-argument to the risk of legal uncertainty and lack of proportionality weighing on the hosting service providers.

In addition, administrative pecuniary sanctions corresponding to a percentage of the turnover would leave the courts more flexible in their judgement and would seem more adaptable to the size of the hosting service providers.

Lastly, the French authorities ask for clarification as to the following wording, which is generally specific to directives, "*Member States shall ensure that a systematic failure to comply with Article 4 (2) is subject to ...*". This wording must imply that Member States are prevented from laying down in their legislation a fine of less than 4%.

Netherlands

The Netherlands would like to stress that it does not unequivocally oppose legislation to prevent the dissemination of online terrorist content. However, any legislation on this area should be effective, and with due respect to the applicable fundamental rights, in particular the freedom of speech and the right to an effective remedy. The Netherlands feels that this balance has not been struck yet in the current text. The main concerns remain the cross-border jurisdiction and its consequences for the legal redress.

The Netherlands retains its parliamentary scrutiny reservation on the entire proposal.[1] It is not expected that the parliamentary scrutiny will be lifted before the December JHA Council, unless our parliament's concerns are adequately addressed.

Cross-border jurisdiction and legal redress

The proposed system of cross-border jurisdiction and the obligation to find legal redress in another Member State, under foreign law, has far-reaching consequences and complications.

Having to seek legal redress before a foreign judicial authority, under foreign national law and in a foreign language, is in the view of the Netherlands not an effective remedy, as required by Article 47 of the Charter on Fundamental Rights, in particular for natural persons and small businesses. Moreover, the Netherlands has concerns about the consequences that a cross-border removal order has for national sovereignty and the protection of fundamental rights, such as the freedom of speech. These concerns remain, as the revised text (14519/18) does not provide for any kind of notification to the receiving Member State, when a removal order is issued to a hosting service provider in its territory.

[1] In addition, our national parliament has filed a motion that urges our government not to agree to any proposal that obligates a Dutch hosting service provider to execute a binding removal order from another Member State, if that removal order is not subject to a national legal remedy.

While examples of cross-border legal proceedings exist, these examples rely on a link to the other Member State concerned, or on a choice of forum. Examples of these proceedings are: committing a (criminal) offence in another Member State; the purchase of goods or services from a seller based in another Member State; or contracts that fall under the scope of the EEX-regulation.[2] In all of these cases there is a link to the state that establishes the jurisdiction. The current text, however, provides each and any Member State in the Union the right to exercise cross-border jurisdiction by the mere fact of issuing a removal order (Article 15 (1) last sentence).

In addition, the current system leads to practical difficulties. Firstly, it does not adequately address the concurrence of multiple removal orders for the same content. It is unclear which Member State has jurisdiction in those circumstances. From the current text it appears that any Member State will have jurisdiction. There are consequently adverse effects for the right to an effective legal remedy – should a HSP or a content provider start legal proceedings in all of the issuing Member States? And if so, how do these procedures relate to each other? There might be divergence in judgments. Secondly, several delegations have already expressed their concerns regarding the risk that a removal order from another Member State could jeopardise running domestic operations, investigations or proceedings.

The current text does not address these issues adequately. Agreements will have to be concluded between Member States, enabling them to cooperate with each other to avoid interference and duplication.[3] While such a system may work in theory, it remains ultimately up to the issuing Member States' exclusive discretion to decide whether or not to actually issue a removal order.

This is exacerbated by the fact that the current proposal contains no guidelines or safeguards regarding the designation of the competent authority. It may be a judicial authority, but Member States may also opt for an administrative body or even a natural person, with no specific safeguards. It is up to such competent authority to assess the content, while it is not always evident what is and what is not terrorist content.

---

2 Regulation 1215/2012/EU of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.

3 In particular with reference to Article 13 of the proposal.

In conclusion: the Regulation offers little guidance on how the fundamental rights will be safeguarded, both in legal and in practical terms.

In view of the above, the Netherlands has suggested a system comparable to that of the GDPR ((EU) 2016/679).

As such, the Netherlands has proposed the following amendment to Article 4 (5).

> (5) The competent authorities shall address a removal order to the competent authority of the Member State where the hosting service provider has its main establishment, or where the legal representative designated by the hosting service provider pursuant to Article 16 resides or is established. The requested competent authority will immediately review and transmit the removal order to the point of contact referred to in Article 14(1). Such orders shall be sent by electronic means capable of producing a written record under conditions allowing to establish the authentication of the sender, including the accuracy of the date and the time of sending and receipt of the order.
>
> The requested competent authority shall not refuse to comply with the request unless:
>
> a. the request is manifestly ill-founded, or
>
> b. compliance with the request would negatively impact national or international criminal or anti-terrorist investigations.

This system ensures that a removal order is always issued by the competent authority of the Member State where the hosting service provider has its main establishment. This proposal avoids cross-border jurisdiction and limits the related issues (where to seek legal redress etc.). This system also ensures that the Member State where the HSP has its main establishment can check for concurrence with national actions (i.e. ongoing criminal investigations in counter-terrorism). At the same time, the suggested marginal review respects the principle of intra-EU trust between Member States of the Union, which presumes that all Member States comply with their obligations under article 47 of the Charter of Fundamental Rights of the European Union. Thus, the legal and practical difficulties that a cross-border judicial procedure creates are alleviated, and by ensuring that only the receiving Member State has jurisdiction, the issue of multiple concurring removal orders is eliminated.

However, this proposal encountered concerns that it may hinder the swift removal of terrorist content.

Although the Netherlands does not share said concerns, it has subsequently - in the spirit of compromise - proposed an alternative, which amends recital 8 and Article 15.

Recital 8 and Article 15:

> Recital 8:
> The right to an effective remedy is enshrined in Article 19 TEU and Article 47 of the Charter of Fundamental Rights of the European Union. Each natural or legal person has the right to an effective judicial remedy before the competent national court against any of the measures taken pursuant to this Regulation, which can adversely affect the rights of that person. The right includes, in particular the possibility for hosting service providers and content providers to effectively contest the removal order. That right can be effectuated before the court of the Member State ~~whose authorities issued the removal order,~~ where the hosting service provider has its main establishment or where the legal representative designated by the hosting service provider pursuant to Article 16 resides or is established.
>
> Article 15 (4)[4]
> An appeal as referred to in Article 4 (9) will be lodged with the court of the Member State where the hosting service provider has its main establishment or where the legal representative designated by the hosting service provider pursuant to Article 16 resides or is established.

[4] Correction of the text of the previous NL proposal (WK 14189/2018 INIT)

The Netherlands feels that this compromise addresses the Commission's and other Member States concerns of delayed removal. It also ensures that content providers, which are often natural persons, in addition to hosting service providers, have an legal remedy available in the Member State where the content is stored, should they feel that content was erroneously removed. And finally, it adequately addresses the issue of shared jurisdiction when multiple removal orders from multiple Member States are being issued for the same piece of content, as all legal proceedings against these removal orders would be under the jurisdiction of a single Member State.

In the recent discussion in the working party, it has been argued that there are legal difficulties with this approach. In particular, it would create difficulties in situations where the competent authority in the issuing Member State is a judicial authority: it would not be possible for a national court to overturn a judicial removal order from another Member State, and the proposed system would negatively impact the national sovereignty of the issuing Member State.

Insofar the proposal would allow the one Member State to exercise jurisdiction over another Member State, the Netherlands would like to clarify that it is due to the proposed Regulation that this perceived issue with cross-border jurisdiction exists. Such a system, and its impact on national sovereignty, is thus inherent to this Regulation and is in fact already in place with the powers to issue a cross-border removal order against a hosting service provider, irrespective of where the hosting service provider has its main establishment.[5]

Secondly, while the issuing competent authority may indeed be a judicial authority, a decision to issue a removal order by such an authority will most likely not be taken in its capacity of a court or tribunal as meant in Article 6 of the Convention for the Protection of Human Rights and Fundamental Freedoms or Article 47 of the Charter of Fundamental Rights of the European Union.

---

5 See in particular Article 15 (1) of the current proposal: "Any Member State shall have jurisdiction for the purposes of Articles 4 and 5, irrespective of where the hosting service provider has its main establishment or has designated a legal representative."

In particular, such a removal order would not be the result of legal proceedings in the common sense of the word, where a defendant (in this case: the content provider and hosting service provider) would appear and plead its case in a public hearing. In fact, the hosting service provider and content provider are not heard at all before a removal order is issued. As such, the decision to issue a removal order would be more akin to an administrative decision than a judicial one, and thus cannot be compared to a regular judicial ruling.

Thirdly, it was suggested that there is no legal basis for overturning a judicial removal order from another Member State. The Netherlands does not feel that this argument holds true, primarily as such a removal order would be more akin to an administrative decision. And secondly, the legal basis for this system would be created and thus found in this Regulation, similar to how the legal basis for a cross-border removal order was created.

Finland

In general, the comments made by Finland in earlier stages continue to apply. Finland still has a general scrutiny reservation. Considering the importance of this piece of legislation and the importance of its effective implementation, Finland would appreciate if a reasonable amount of time was given to consider the changes made by the Presidency and proposals made by other Member States.

Below you will find some concrete, but preliminary, text proposals.

Article 2 - Definitions

The definitions should be clear and precise. The definitions should also, as far as possible, be consistent with other EU legislative instruments in order to not to create confusion among the public.

Hosting service provider

Finland is of the opinion that the revised recital 10 will lead to a situation where the responsibility to act would be primarily on the civil society actors or on small and medium size companies. Although Finland does understand that there should be no safe havens to disseminate terrorist content, the one-hour rule to react 24/7 would be a disproportionate burden especially for civil society actors and for small and medium companies. The primary responsibility to act should not be place to these actors. It seems that in different EU legislation the hosting service provider is defined differently:

The *E-Commerce Directive* 2000/31/EC and the subsequent EU case law have defined the service provider. Art 2 of the E-Commerce Directive defines 'information society services' and 'service provider'. In addition, the case law of the EU Court of Justice (C-236/08 - C-238/08 and C-324/09) has stated that the role of the hosting service provider is *neutral, its services are purely technical, automatic and passive*, which means that it is not aware of the information stored in its service. The hosting service provider does not monitor the content or information either.

Also the current version of the *e-Evidence Regulation* (Art 3 para 3b) seems to emphasize the storage of data as a defining component of the service.

Finland asks to note the definition of "online content sharing service provider" of the Copyright Directive:

(5) 'online content sharing service provider' means a provider of an information society service whose main or one of the main purposes is to store and give access to the public to a significant amount of copyright protected works or other protected subject-matter uploaded by its users, which the service organises and promotes for profit making purposes. Microenterprises and small-sized enterprises within the meaning of Title I of the Annex to Commission Recommendation 2003/361/EC and services acting in a non-commercial purpose capacity such as online encyclopaedia, and providers of services such as non-for-profit online encyclopaedias, non-for-profit educational and scientific repositories, non-for-profit open source software developing platforms, as well as internet access service providers, online marketplaces and providers of cloud services which allow users, including businesses for their internal purposes, to upload content for their own use shall not be considered online content sharing service providers within the meaning of this Directive.

Finland proposes the following changes to Article 2 para 1 and 6, as well as new paras 10 and 11 defining content data and terrorist content data. The aim is to make the definition of *'hosting service provider'* clearer and more aligned with e-commerce and E-evidence legislation.

COM proposal	Presidency proposal	Finnish proposal
Article 2		
(1)'hosting service provider' means a provider of information society services consisting in the storage of information provided by and at the request of the content provider and in making the information stored available to third parties;	(1)'hosting service provider' means a provider of information society services consisting in the storage of information provided by and at the request of the content provider and in making the information stored available to third parties;	(1)'hosting service provider' means a provider of information society services consisting in the ***technical, automatic and passive*** storage of ~~information~~ ***content data*** provided by and at the request of the content provider and in making the information stored available to third parties;
		(6)'dissemination of terrorist content' means making terrorist content available to

		third parties on the hosting service providers' services;
		New para 10 and 11 **(10) 'content data' means data that is stored in a digital format such as text, voice, videos, images, and sound other than subscriber, access or transactional data** **(11) 'terrorist content data' means data that contains terrorist content referred to in paragraph 5 and is stored in a digital format such as text, voice, videos, images, and sound other than subscriber, access or transactional data;**

Terrorist Content

Definition on terrorist content is developing in a better direction. Finland proposes some amendments. In paragraph 5 a Finland prefers to refer to "terrorist offences" and not "terrorist acts". Terrorist acts are not defined or addressed in this Regulation.

COM proposal	Presidency proposal	Finnish proposal
Article 2	Article 2	Article 2
(4) 'terrorist offences' means offences as defined in Article 3(1) of Directive (EU) 2017/541; (5) 'terrorist content' means one or more of the following information: (a) inciting or advocating, including by glorifying, the commission of terrorist offences, thereby causing a danger that such acts be	(4) 'terrorist offences' means offences as defined in Article 3(1)~~(a)-(i)~~ of Directive (EU) 2017/541; (5) 'terrorist content' means ~~*one of the following*~~ ***types of*** ~~*information*~~ ***material*** **which may contribute to the commission of terrorist offences, as defined in Article 3(1)(a) to (i) of the Directive 2017/541, by**:	(4) 'terrorist offences' means offences as defined in Article 3(1)**(a)-(i)** of Directive (EU) 2017/541; (5) 'terrorist content' means ~~*one of the following*~~ ***types of*** ~~*information*~~ ***material*** **(a) containing a threat to commit a terrorist offence;** **(b) inciting and advocating, such as by the glorification of terrorist acts, the**

committed; (b) encouraging the contribution to terrorist offences; (c) promoting the activities of a terrorist group, in particular by encouraging the participation in or support to a terrorist group within the meaning of Article 2(3) of Directive (EU) 2017/541; (d) instructing on methods or techniques for the purpose of committing terrorist offences.	**(aa) threatening to commit a terrorist offence;** (a) inciting or advocating, ~~including~~ **such as** ~~by glorifying~~ **the glorification of terrorist acts,** the commission of terrorist offences, thereby causing a danger that such acts be committed; **(b) soliciting persons or a group of persons to commit or**~~encouraging the~~ contribut**e**~~ion~~ to terrorist offences; (c) promoting the activities of a terrorist group, in particular by **soliciting persons or a group of persons to** ~~encouraging the~~ participat**e**~~ion~~ in or support **the criminal activities of** ~~to~~a terrorist group within the meaning of Article 2(3) of Directive (EU) 2017/541; (d) instructing on methods or techniques for the purpose of committing terrorist offences.	**commission of terrorist offences, thereby causing a danger that one or more such offences may be committed; or** **(c) contributing to the commission of a terrorist offence** **- by supplying information to a terrorist group defined in Article 2(3) of Directive (EU) 2017/541;** **- by soliciting another person to commit such an offence; or** **- by providing instruction on the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or on other specific methods or techniques.**

Cooperation - Consultation Procedure, New Article X

It would be important to add that when a competent authority in one Member State makes a removal order or referral, it should at least inform the contact point of the other Member State where the hosting service provider has its main establishment. The issuing Member State could choose to use for example Europol to transmit the copy of the removal order or referral as referred to in Article 13.

Finnish proposal
New Article X on Consultation procedure
1. The issuing authority shall submit a copy of the removal order or referral to the competent authority referred to in Article 17(1 a) of the Member State in which the main establishment of the hosting service provider is located at the same time it is transmitted to the hosting service provider in accordance with Article 4 (5). **2. In cases where the competent authority of the Member State in which the main establishment of the hosting service provider is located has reasonable grounds to believe that the removal order may impact fundamental interests of that Member State, it shall inform the issuing competent authority.** **3. The issuing authority shall take these circumstances into account in the same way as if they were provided for under its national law and shall withdraw or adapt the removal order or referral where necessary to give effect to these grounds.**

Referrals - Article 5

Finland proposes to amend Article 5 paragraph 4 so that it is aligned with Article 2 paragraph 8 which defines referrals.

Finnish proposal
Article 5 Referrals
4. The referral shall contain sufficiently detailed information, including on the reasons why the content ~~is~~ **may be** considered terrorist content, and provide a URL and, where necessary, additional information enabling the identification of the terrorist content referred.

Preservation of data - Articles 7 and 2

In order to make it clearer what sort of data the HSP is to preserve, Finland proposes the following amendments.

The HSP's should preserve terrorist content data as well as available related subscriber data, access data and transactional data. Article 7 should state that the data should be preserved but only if it is available for the HSP. In Article 2; subscriber data, access data and transactional data could be defined in accordance with e-Evidence Regulation. Furthermore, related data is not required to be removed based on a removal order, and therefore Finland proposes to delete text in paragraph 1 (that suggests that the related data should be removed).

The HSP's are not in a position to estimate what type of data is necessary for administrative proceedings, investigation or prosecution etc. referred to in para 1 a-b. Therefore, Finland proposes to delete the words "and which is necessary". The HSP's should in general preserve terrorist content data as well as available related subscriber data, access data and transactional data.

In paragraph 2 Finland proposes to include the possibility to continue the preservation time also for detection, investigation and prosecution of terrorist offences.

COM proposal	Presidency proposal	Finnish proposal
Article 7 Preservation of content and related data	Article 7 Preservation of content and related data	Article 7 Preservation of content **data** and related data
1. Hosting service providers shall preserve terrorist content which has been removed or disabled as a result of a removal order, a referral or as a result of proactive measures pursuant to Articles 4, 5 and 6 and related data removed as a consequence of the removal of the terrorist content and which is necessary for: (a) proceedings of administrative or judicial review, (b) the prevention, detection,	1. Hosting service providers shall preserve terrorist content which has been removed or disabled as a result of a removal order, a referral or as a result of proactive measures pursuant to Articles 4, 5 and 6 and related data removed as a consequence of the removal of the terrorist content, and which is necessary for: (a) proceedings of administrative or judicial review, (b) the prevention, detection,	1. Hosting service providers shall preserve terrorist content **data** which has been removed or disabled as a result of a removal order, a referral or as a result of proactive measures pursuant to Articles 4, 5 and 6 and **available** related **subscriber data, access data and transactional** data ~~**removed as a consequence of the removal of the terrorist content, and which is necessary**~~ for: (a) proceedings of administrative or judicial

investigation and prosecution of terrorist offences. 2. The terrorist content and related data referred to in paragraph 1 shall be preserved for six months. The terrorist content shall, upon request from the competent authority or court, be preserved for a longer period when and for as long as necessary for ongoing proceedings of administrative or judicial review referred to in paragraph 1(a). 3. Hosting service providers shall ensure that the terrorist content and related data preserved pursuant to paragraphs 1 and 2 are subject to appropriate technical and organisational safeguards. Those technical and organisational safeguards shall ensure that the preserved terrorist content and related data is only accessed and processed for the purposes referred to in paragraph 1, and ensure a high level of security of the personal data concerned. Hosting service providers shall review and update those safeguards where necessary.	investigation and prosecution of terrorist offences. 2. The terrorist content and related data referred to in paragraph 1 shall be preserved for six months. The terrorist content shall, upon request from the competent authority or court, be preserved for a longer period when and for as long as necessary for ongoing proceedings of administrative or judicial review referred to in paragraph 1(a). 3. Hosting service providers shall ensure that the terrorist content and related data preserved pursuant to paragraphs 1 and 2 are subject to appropriate technical and organisational safeguards. Those technical and organisational safeguards shall ensure that the preserved terrorist content and related data is only accessed and processed for the purposes referred to in paragraph 1, and ensure a high level of security of the personal data concerned. Hosting service providers shall review and update those safeguards where necessary.	review, (b) the prevention, detection, investigation and prosecution of terrorist offences. 2. The terrorist content **data** and related data referred to in paragraph 1 shall be preserved for six months. The terrorist content **data and related data** shall, upon request from the competent authority or court, be preserved for a longer period when and for as long as necessary for ongoing proceedings of administrative or judicial review **or for the detection, investigation and prosecution of terrorist offences** referred to in paragraph 1~~**(a).**~~ 3. Hosting service providers shall ensure that the terrorist content **data** and related data preserved pursuant to paragraphs 1 and 2 are subject to appropriate technical and organisational safeguards. Those technical and organisational safeguards shall ensure that the preserved terrorist content **data** and related data is only accessed and processed for the purposes referred to in paragraph 1, and ensure a high level of security of the personal data concerned. Hosting service providers shall review and update those safeguards where necessary.
Article 2	Article 2	**Article 2 new paragraphs 12-14** in accordance with E-Evidence Reg Art 2 paras 7-10 (version of 19 Nov 2018,

		1213/4/18 RVE 4)
		(12) 'subscriber data' means any data pertaining to: **(a) the identity of a subscriber or customer such as the provided name, date of birth, postal or geographic address, billing and payment data, telephone, or email;** **(b) the type of service and its duration including technical data and data identifying related technical measures or interfaces used by or provided to the subscriber or customer, and data related to the validation of the use of service, excluding passwords or other authentication means used in lieu of a password that are provided by a user, or created at the request of a user;** **(13) 'access data' means data related to the commencement and termination of a user access session to a service, which is strictly necessary for the sole purpose of identifying the user of the service, such as the date and time of use, or the log-in to and log-off from the service, together with the IP address allocated by the internet access service provider to the user of a service, data identifying the interface used and the user ID. This includes electronic communications metadata as defined in point (gc*)* of**

		Article 4(3) of [Regulation concerning the respect for private life and the protection of personal data in electronic communications]; **(14) 'transactional data' means data related to the provision of a service offered by a service provider that serves to provide context or additional information about such service and is generated or processed by an information system of the service provider, such as the source and destination of a message or another type of interaction, data on the location of the device, date, time, duration, size, route, format, the protocol used and the type of compression, unless such data constitues access data. This includes electronic communications metadata as defined in point (gc) of Article 4(3) of [Regulation concerning the respect for private life and the protection of personal data in electronic communications];**

Points of contact – Article 14

In relation to article 14, we support the comments made by DE in relation to recital 33 (establishment of 24/7 PoC only for those HSPs that have been exposed to terrorist content). Considering that the Regulation is directly applicable, Finland would prefer to have this limitation also written in the Article itself.

(33) Both hosting service providers and Member States should establish points of contact to facilitate the swift handling of removal orders and referrals. In contrast to the legal representative, the point of contact serves operational purposes. The hosting service provider's point of contact should consist of any dedicated means**, inhouse or outsourced,** allowing for the electronic submission of removal orders and referrals and of technical ~~and~~ **or** personal means allowing for the swift processing thereof. The point of contact for the hosting service provider does not have to be located in the Union and the hosting service provider is free to nominate an existing point of contact, provided that this point of contact is able to fulfil the functions provided for in this Regulation. With a view to ensure that terrorist content is removed or access to it is disabled within one hour from the receipt of a removal order, hosting service providers **who have already received a removal order or referral and still are exposed to terrorist content** should ensure that the point of contact is reachable 24/7. **Hosting service providers who have not been misused for disseminating terrorist content yet or are not exposed to terrorist content any more should ensure that the point of contact is at least reachable 8/5.** The information on the point of contact should include information about the language in which the point of contact can be addressed. In order to facilitate the communication between the hosting service providers and the competent authorities, hosting service providers are encouraged to allow for communication in one of the official languages of the Union in which their terms and conditions are available.

Sweden

Sweden welcomes the proposal for a new article 1.3. making it unequivocal that the Regulation will not have the effect of modifying the obligations to respect fundamental rights, as enshrined in Article 6 of the treaty of the European Union. However, it is still of utmost importance for us with a similar reference to fundamental principles relating to the freedom of expression, the freedom of the press and the freedom and pluralism of the media.

Proposal for additional point to Article 1 of the proposed Regulation

Article 1

Subject matter and scope

…

4. Member states may establish conditions required by, and in accordance with, fundamental principles relating to the freedom of the press and other media, governing the rights and responsibilities of, and procedural guarantees for, the press or other media.

…

Rationale

1. This will align Article 1 of the proposed Regulation with Article 23 of the Directive (2017/541) on combating terrorism as regards fundamental rights and freedoms.
2. It is imperative for Sweden that the freedom of the press and the freedom and pluralism of the media can be upheld:

Freedom of expression and the freedom and pluralism of the media is a very special concern for Sweden and we have a completely separated legal framework for the protection of freedom of speech in constitutionally protected mediums, i.e. newspapers, radio, TV and also certain publications online. If a webpage is protected under our Fundamental law on the freedom of expression public authorities cannot intervene against publications on the webpage other than in those cases and in the manner laid down in the fundamental law.

An effect to this is that the public can not restrict access to content on a constitutionally protected webpage in the area that is protected by the fundamental law. There is also an absolute ban on any sort of preview imposed by the public for publications on such webpages. Measures due to content on a constitutionally protected webpage can only be taken against an appointed responsible editor who takes full responsibility for the publications.

Publications online can only be protected by our fundamental law on the freedom of expression in cases where traditional media with a responsible editor is acting online or if an online publication applies for a "certificate of publication" and reports a responsible editor. The protection also requires that the content on the webpage only can be changed by the person who runs the business. As a consequence, social media platforms and other platforms/ where people can upload their own material can never gain the certain protection under the fundamental law. The vast majority of online publication is also not protected by our fundamental law on the freedom of expression. However, traditional media and webpages with a "certificate of publication" sometimes act through hosting service providers, and in those cases we need to ensure that we fully can uphold the special principles in our fundamental law.

In order to ensure that we can uphold our fundamental legal system for the protection of the freedom of the press, and the freedom and pluralism of the media we therefore need article 1 to include some sort of reference to fundamental principles relating to the freedom of expression, the freedom of the press and the freedom and pluralism of the media.

Additional comments as regards Article 1 of the proposed Regulation

In addition to what is stated above, Sweden welcomes and supports the German proposal for a recital linked to Article 1 as pronounced during the meeting:

content that is attributable or disseminated under the editorial responsibility of a provider governed by standards in line with union law shall be exempt from scope of this regulation

In addition to what is stated above, Sweden similarly welcomes and supports the German proposal for additional text in Article 2(5):

In terms of this regulation 'terrorist content' shall not mean content published under the editorial responsibility of a content provider based on journalistic standards established by press or media regulation consistent with the law of the Union.

United Kingdom

1) National Security Competence

The UK submitted text on this earlier in the week and raised during TWP discussions today. The Commission and Presidency mentioned that it would be helpful to see further reasoning of why we are suggesting this inclusion. As such, we thought it would be useful to flag some precedents of other regulations that have included similar text on National Security competence (none of which have a JHA legal base). We want to remain consistent with other regulations. Please see examples below:

(a) This regulation reflects and is consistent with similar provisions, in recital (16) and Art 2(2) of the General Data Protection Regulation. Recital (16) says "This Regulation does not apply to … the free flow of personal data related to activities which fall outside the scope of Union law, such as activities concerning national security." And Art 2(2)(a) says: "This Regulation does not apply to the processing of personal data: (a) in the course of activities that fall outside the scope of Union law;"

(b) This regulation reflects and is consistent with similar provisions, in Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (adopted in July 2016) in Article 1(6):

"This Directive is without prejudice to the actions taken by Member States to safeguard their essential State functions, in particular to safeguard national security, [*including actions protecting information the disclosure of which Member States consider contrary to the essential interests of their security, and to maintain law and order, in particular to allow for the investigation, detection and prosecution of criminal offences.*]"

(c) Art 4(2) TEU: 'national security remains the sole responsibility of each Member State.'

(d) This regulation reflects and is consistent with similar provisions in the draft ePrivacy Regulation.

- Article 2 : (a) activities which fall outside the scope of Union law; (aa) activities concerning national security and defence;

- Recital 7a : This Regulation should not apply to the protection of fundamental rights and freedoms regarding activities concerning national security and defence.

Further to these examples, we have suggested more succinct text below (compared to our original submission on Tuesday) should that be easier to include in the draft text. We would like to see text on competence included in the operative part of the text.

Recital:

START

This Regulation does not regulate in any way the activities of Member States which fall outside the scope of Union law and in any case to activities in relation to national security. [More specifically, this Regulation does not put in place any additional restrictions, obligations or requirements in respect of access to content removed by online service providers who have hosted such content, or data and information processed by those providers relating to the removed content]. **END**

Article 1(4) (repeat)

START

This Regulation does not regulate in any way the activities of Member States which fall outside the scope of Union law and in any case to activities in relation to national security.

END

2) **Recital 13**

The UK still retains concerns regarding the issue of "disabling access". While we welcome the Presidency's attempts at further clarity in Recital 13, the proposed text suggests disabling access merely means making access difficult to achieve, which is a much lower bar than UK and French suggested text. One can envisage a situation where an HSP would say that access has been disabled but where we would say that what has been done is so straightforward to circumvent that they have not in reality disabled access. The text in the recital would make it difficult to argue that disabling access goes beyond what the recital says. We ask the Presidency to reconsider previously submitted text on this issue.

3) **Recital 27**

The UK has noted the amendment to Recital 27. While we appreciate the Commission's explanation at TWP today, we still have substantial concerns that consulting all Member States (even via Europol) before issuing a removal order would significantly slow down the removal order process, which ultimately goes against the objective of the regulation - taking down terrorist content within one hour. We have particular concerns about doing this for referrals, which is currently not common practice between IRUs of Member States and Europol. As such, the UK does not support the amendment and wishes the text to revert to the original wording:

"..when issuing removal orders or sending referrals"

If this is very problematic for other Member States, at the very least we would want to exempt referrals from this process and limit deconfliction to removal orders. As such, fall back to the following text:

"..***when issuing referrals or before*** issuing removal orders"

4) **Article 2**

The UK is content with the amendments to Article 2(5). We also welcome the change to Article 2(4) to include all of the offences in Article 3(1) of Directive 2017/541 - including threats to commit the other offences. However, we would like to highlight that Article 3(1) does not actually define "terrorist offences". It lists acts which member states must define as terrorist offences where they are committed with one of the aims in article 3(2) of Directive 2017/541. For the benefit of clarity it may be better to properly reflect the drafting of Directive 2017/541 for example, by saying something similar to:

"terrorist offences means one of the intentional acts listed in Article 3(1) of Directive 2017/541)".

5) Article 13(4)

The UK previously submitted drafting changes to this paragraph due to our concern that as drafted, the companies will be tempted to send information to the easiest point of contact (namely their Member State of legal jurisdiction) rather than the Member State who would be concerned by the information. We understand colleagues raised concerns with our suggested text and as such have provided alternative wording below which we hope gets round the risk of a Member State being flooded with notifications which they would then have an obligation to action.

> Where hosting service providers become aware of any evidence of terrorist offences ~~**[within the meaning of Article 3 of the Terrorism Directive]**~~ they shall promptly inform authorities competent for the investigation and prosecution in criminal offences in the concerned Member State**(s)**. ~~**or the point of contact in the Member State pursuant to Article 14(2), where they have their main establishment or a legal representative.**~~ **Where it is impossible to identify the Member State(s) concerned, the h**~~H~~osting service providers **shall notify the point of contact in the Member State pursuant to Article 14(2), where they have their main establishment or a legal representative, and** may **also**~~, in case of doubt,~~ **also** transmit this information to Europol for appropriate follow up.

6) Article 14 / Recital 33

Colleagues intervened during discussions today to suggest that "first time offenders" should not be expected to have a 24/7 contact point until their first misuse.

The UK believes it is vital that HSPs of every size respond to terrorist content on their platforms within the shortest possible time to prevent further dissemination of such content. We are concerned that allowing 'first time offenders' longer to respond would undermine the spirit of the Regulation (removing content at pace) and would mean that HSPs are disincentivised from making the necessary preparations, including in terms of resourcing. As such, we would not support an amendment to **Article 14.**

However, we do understand that less well-resourced HSPs may face greater difficulty in responding within one hour and requiring an HSP that has never received a removal order or referral to maintain a 24/7 point of contact may be disproportionate. As such, if there is a strong opinion amongst Member States, we would be able to support a minor amendment to **Recital 33**, such as:

> "With a view to ensure that terrorist content is removed or access to it is disabled within one hour from the receipt of a removal order, hosting service providers that have previous received a removal order [or referral] should ensure that the point of contact is reachable 24/7."

7) **Article 15**

   - UK is content with addition in paragraph 1
   - UK is content with deletion of paragraph 3
   - With regards to the jurisdiction and legal redress of removal orders, the UK is currently content with the regulation as drafted.

8) **Article 18/Recital 38** – no comments. Content with current text.